Cyber Security Centre for the Isle of Man

CLASSIFICATION: TLP CLEAR

ISLE OF MAN CYBER THREAT UPDATE

January - February 2025

INTRODUCTION

For the period 1st January - 28th February

Welcome to the latest edition of the Cyber Threat Update brought to you by the Cyber Security Centre for the Isle of Man (CSC), a part of OCSIA. This document provides an overview of cyber threats using data collected from our reporting points as well as intelligence obtained from partner agencies and open-source services.

We can only offer advice and guidance based on the information we have. Therefore, if you have any information that you believe should be considered for this document, please reach out to us at cyber@gov.im or submit it via our online cyber concerns form.

CONTENTS

Suspicious Email Reporting Service (SERS)	**1**
Reported Cyber Concerns	**3**
Isle of Man Threat Commentary	**5**
External Threat Commentary	**10**
Cyber Glossary	**15**
About Us	**17**

SUSPICIOUS EMAIL REPORTING SERVICE (SERS)

As part of the Isle of Man Government's Cyber Security Strategy, the Cyber Security Centre for the Isle of Man (CSC) operates a Suspicious Email Reporting Service (SERS), allowing residents to forward suspicious emails for analysis.

If you have received an email which you're not quite sure about, forward it to SERS@ocsia.im. The message might be from a company that you don't normally receive communications from or from someone that you do not know. You may just have a hunch. If you are suspicious about an email, you should report it.

Your report of a suspicious email will help us to act quickly, protecting many more people from being affected. In a small number of cases, an email may not reach our service due to it already being widely recognised by spam detection services.

By sending your suspicious emails to us we can better understand the threats on our Island and provide relevant advice and warnings. Your email will also be analysed by the UK's National Cyber Security Centre (NCSC), assisting in the disruption of malicious phishing campaigns and take down of websites.

The National Cyber Security Centre (NCSC) has the power to investigate and remove scam email addresses and websites. By reporting phishing attempts you can:

- reduce the amount of scam emails you receive
- make yourself a harder target for scammers
- protect others from cyber crime online

Since the launch of SERS, we have received over 27,400 suspicious emails. In January and February 2025, we received 1,331 suspicious emails.

SUSPICIOUS EMAILS

1,331 REPORTED

in January and February

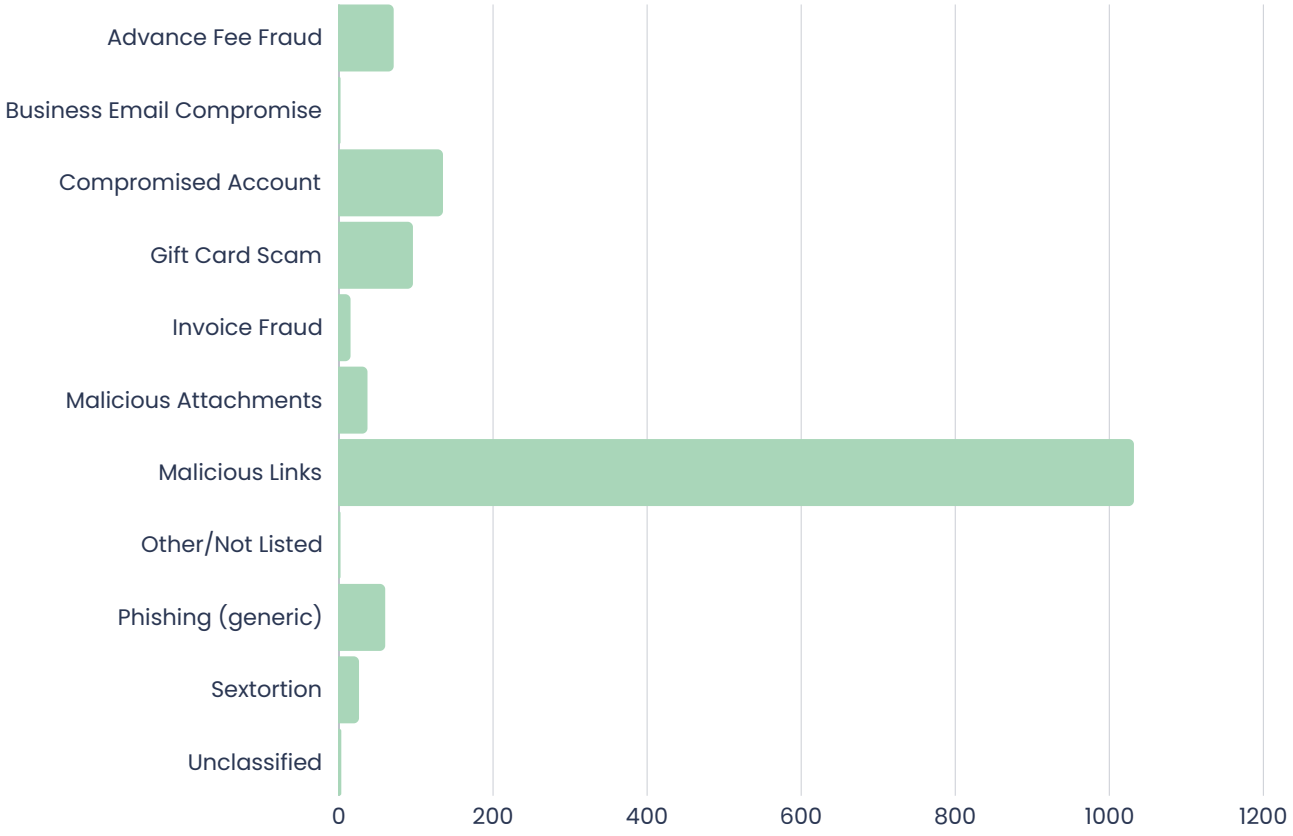
Detail

The graph below shows the frequency of specific characteristics identified in submitted SERS emails. Please note that some emails have more than one recorded characteristic.

Whilst malicious links do make the bulk of submissions as usual, this period is notable for the increased prevalence of other suspicious emails

Top 5 Phishing Scams Imitating Popular Services:

1. Manx.net
2. Romance and dating
3. PayPal
4. Parcel Delivery
5. Anti-malware Software



CYBER CONCERNS

98 REPORTED

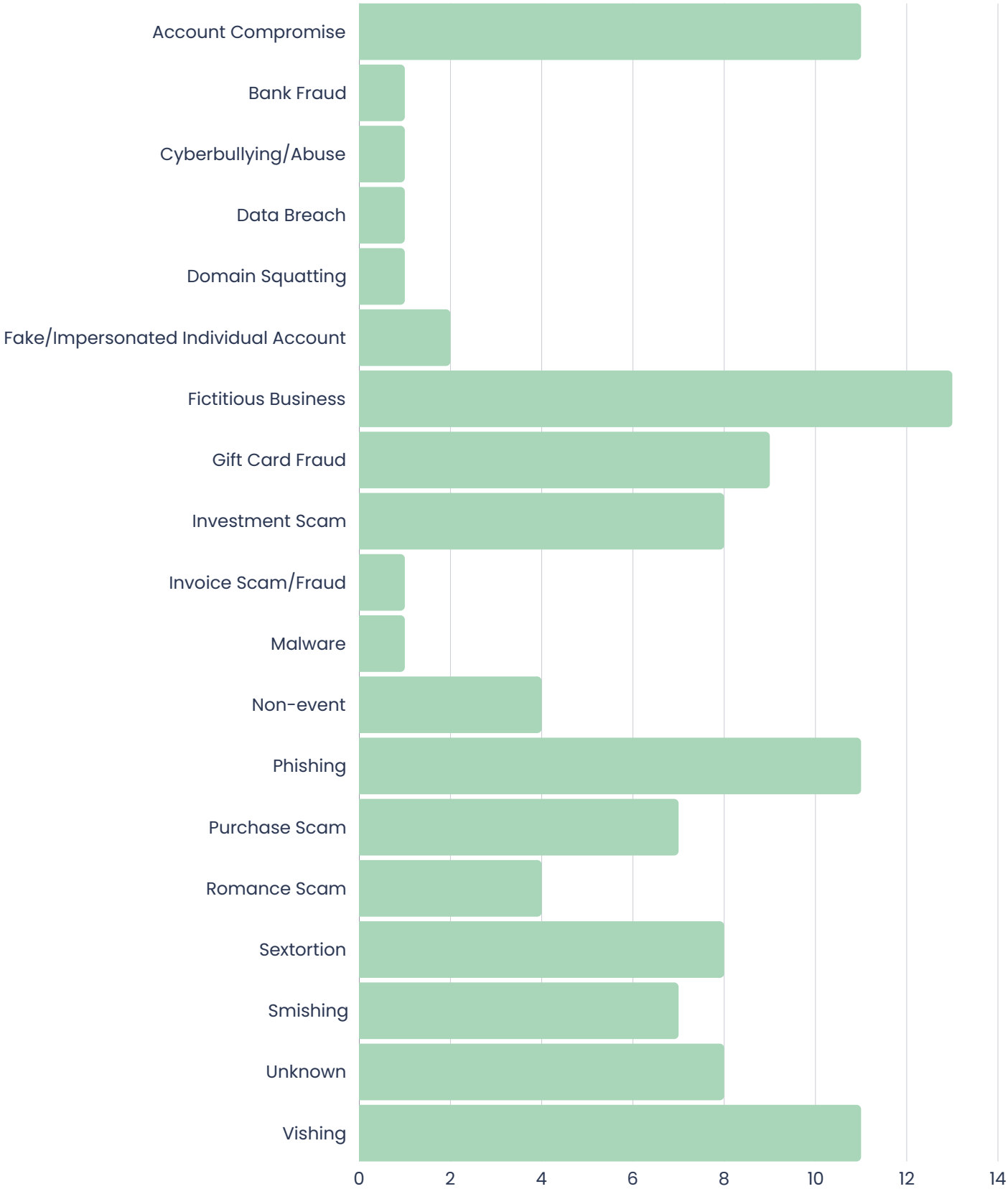
in January and February

Detail

The chart (on page 4) shows a breakdown of cyber concerns reported to us over January and February.

As mentioned previously, we can only provide the right advice and guidance to the public and local businesses from the information that is shared and reported to us. It is, therefore, important that we receive reports from the public and from organisations. If anyone has any information that they wish to put forward for consideration that could contribute to this document, please contact us at cyber@gov.im or report it using our online cyber concerns form.

Cyber Concerns January and February



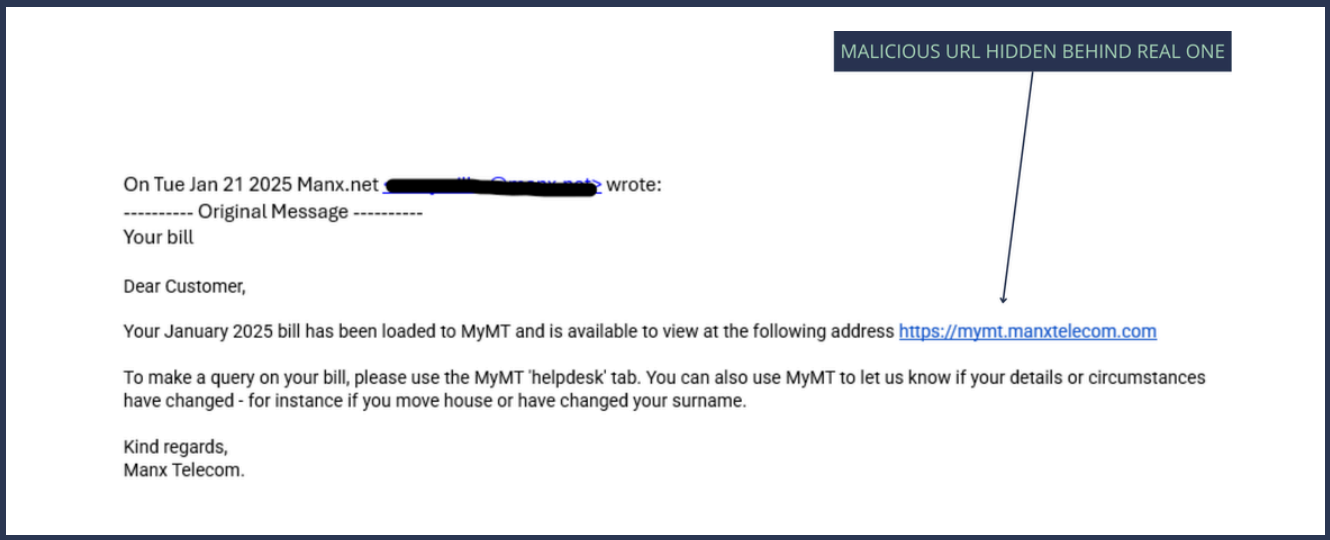
ISLE OF MAN THREAT COMMENTARY

ACCCOUNT COMPROMISE

MANX NET CONTINUES...

We have previously referenced the number of Manx.net scam emails in a large co-ordinated phishing campaign. The emails encouraged users to submit login details which when entered granted the criminals access to the victim's account. We have discussed Manx.net at length and are pleased to see that in March (at the time of writing) the number of SERS submissions have decreased.

However, it is worth noting that these emails did continue over the period and criminals adapted their tactics to target those not fooled by the first round of emails. An example of this included adapting the emails to look like notifications for legitimate Manx Telecom Bills, which utilised a malicious link hidden behind the actual Manx Telecom e-billing platform, a number of account compromises did occur as a result of this.



Scam email with the obfuscated link

INVESTMENT SCAMS

A victim, in the process of relocating from the island to the UK, was searching for investment opportunities. During the search, they came across an online investment scheme that appeared promising. After clicking on a link related to the scheme, they were contacted by a woman named Wendy, who became her main point of contact for the investment. Wendy seemed professional and convincing, offering the victim the opportunity to grow her funds. Initially, the victim invested £188 into the scheme. Encouraged by Wendy's reassurances and the apparent success of the investment, they then made progressively larger investments, totalling £2,000, then £10,000, and eventually £100,000.

However, the victim was then informed that she owed a tax bill related to her investments. Faced with a lack of available funds, they took out a loan with a bank for £22,000 to cover the payment. Still needing more funds, they approached friends for further loans, borrowing £31,400 and £33,000. Despite these efforts, they were still short of the money needed, so she turned to another friend for an additional £22,000. It was at this point that her friend raised concerns and investigated the situation, ultimately informing the victim that it was a scam. Realising she had been deceived, the victim reported the matter to Barclays Bank on January 24, 2025. The bank passed the case to their fraud team, where an employee confirmed that the scheme was indeed a scam and advised them to report the matter to the police.

This experience has highlighted the dangers of unverified online investments and the importance of scepticism when promises of quick financial returns are made. The involvement of friends in uncovering the truth shows the importance of having a support network that can provide an objective perspective during potentially stressful situations. The case also illustrates the lengths to which scammers will go to exploit individuals, reinforcing the need for vigilance and thorough research before engaging in financial ventures, particularly those that seem too good to be true.

IMPERSONATED ACCOUNT OR PROFILE (INDIVIDUAL)

CELEBRITY IMPERSONATION

For a considerable period of time, a victim had been in communication via social media with a profile who they believed to be a celebrity singer.

The scammer then socially manipulated the victim, encouraging them to send money for various reasons. With the victim supplying this money to accounts provided by the scammer. This developed further, with PayPal and additional bank accounts opened in order to facilitate these payments.

The scam, which had been occurring over a period of months, was only discovered when the victim began borrowing money from different family members to fund the payments.

The total loss is believed to be between £700-£800

PHISHING

MICROCHIPPED CATS

A pet owner received two emails, one for each of their cats, claiming that their microchip registration had expired and urging immediate renewal. The emails included accurate microchip numbers and contact details, which made them appear legitimate. However, after checking with their veterinarian, the owner learned that microchip registrations do not expire, and the emails came from a company unrelated to the microchip registries for their pets. This led the owner to suspect the emails were scams.

The accuracy of the information raised concerns about a potential data breach. It's likely the scammer gained access to the pet owner's details, such as microchip numbers, possibly from a breach from a third-party source. This data was used to craft a convincing phishing attempt.

SEXTORTION

SHARING OF EXPLICIT IMAGES

A case was reported by a victim, who had been targeted through a series of social engineering tactics, leading to extortion and financial loss. The incident began when they received a message on Instagram from an account named "BECKYLOUISE907," which appeared to have mutual friends. Initially, the interaction seemed innocuous, but it quickly escalated as the account began sharing explicit images of themselves and encouraged them to reciprocate by sending explicit images in return.

The conversation shifted to WhatsApp, where the victim was contacted by a number +44 7728 466168. Although the interaction seemed suspicious, the victim continued the conversation. However, the situation escalated when they received a message from a separate WhatsApp number, starting with the country codes +243 or +234 (Congo/Nigeria). The message contained a threat that if they did not pay a specified amount of money, the explicit images would be released to the public. This threat was further compounded by the creation of an Instagram group chat that included some of the victims followers and family members, increasing the pressure and intimidation.

The perpetrators conducted thorough social engineering by researching the victim's background, using personal information to further manipulate and coerce them into complying with their demands. The extortionists provided payment details for an account based in Kazakhstan.

Sextortion is a rising trend, with well-organised gangs actively targeting the UK and Isle of Man. The problem is becoming so widespread (particularly among teenage boys) that the National Crime Agency have recently launched a campaign to raise awareness of the issue.

SMISHING

‘HEY MUM’ MESSAGES

A recent case of a potential scam was reported to the police after a complainant received a WhatsApp message from what appeared to be her son. The message requested that she note down a new mobile number, 07523 597860. The person then claimed they needed £950 to purchase a new mobile phone, which the complainant promptly transferred to an account via a bank transfer. However, after contacting her real son, he called the number and discovered it was a man with a Manchester accent. When he confronted the individual, asking for the money to be returned, the scammer responded callously, saying, "IT'S MY JOB, I DO MANY OF THESE EACH DAY, I DON'T KNOW WHICH ONE IS YOUR MUM." The complainant’s case highlights the growing threat of such scams, particularly those involving WhatsApp or text message campaigns that are designed to create a sense of urgency and prey on emotions.

These scams have become more prevalent in recent times, with many Manx residents reporting similar incidents. Scammers frequently impersonate family members or financial institutions to exploit people's vulnerabilities. A common tactic involves pretending to be a child or relative asking for money to replace a broken phone. Others may pose as representatives of banks or credit card departments, warning recipients about suspicious transactions on their accounts.
To protect from falling victim to such scams, it is crucial to remain cautious when receiving messages from unknown numbers. If you receive a message that seems suspicious or unexpected, do not respond immediately. Instead, read the message carefully and check for any inconsistencies in the tone or style of writing compared to how you would expect a friend, family member, or business to communicate. You should always contact people you know using verified contact information rather than relying on the number provided in the message.

EXTERNAL THREAT COMMENTARY

SOUTHERN WATER FACES £4.5 MILLION FALLOUT FROM BLACK BASTA RANSOMWARE ATTACK

In March 2025, fresh details have emerged regarding the severe financial impact of a ransomware attack suffered by Southern Water. The cyberattack, which was carried out by the Black Basta ransomware group in February 2024, has now been confirmed to have cost the utility company more than £4.5 million in expenses. This latest revelation underscores the ongoing financial burden imposed on the organisation well over a year after the initial breach.

According to information published by Bleeping Computer and other cybersecurity sources, Southern Water had to engage external cybersecurity experts and legal advisors to mitigate the damage caused by the attack. Although the incident compromised a portion of the company's IT systems, Southern Water has consistently reassured customers that essential services, including water supply and wastewater management, were not disrupted. However, reports indicate that data belonging to around 10% of its customer base was affected, raising concerns over potential leaks.

New information emerging in 2025 suggests that Southern Water has continued to monitor the dark web for signs of stolen data being circulated. The company has also been working closely with regulatory authorities and cybersecurity specialists to enhance its digital defences and prevent future attacks.

TALKTALK INVESTIGATES DATA BREACH AMID DISPUTED IMPACT ASSESSMENTS

TalkTalk, the UK telecommunications provider, is currently investigating a data breach involving a third-party supplier's system. A hacker known as 'b0nd' has claimed to have stolen the personal data of approximately 18.8 million current and former customers in January 2025. The compromised information allegedly includes names, email addresses, last-used IP addresses, and phone numbers.

However, TalkTalk has disputed these figures, stating that the number of affected customers is "wholly inaccurate and significantly overstated." The company has clarified that no billing or financial information was involved in the breach and that it is believed to have originated from CSG Ascendon's subscription management platform. Despite these claims, CSG Ascendon denies any direct compromise of its technologies.

Both TalkTalk and CSG Ascendon are conducting their own investigations to determine the full scope of the incident. This case highlights the growing vulnerabilities associated with third-party supply chains and underscores the critical importance of robust vendor risk management practices in protecting sensitive customer data.

UK GOVERNMENT FACES GROWING CYBER THREATS, NAO WARNS OF INCREASING VULNERABILITIES

A recent report by the National Audit Office (NAO) warns that the UK government's cyber security is under significant threat, with growing risks from hostile cyber actors. Despite a decade-long push for stronger defences, vulnerabilities persist in many departments, especially in outdated IT systems that remain unprotected. As of 2024, 228 'legacy' systems are in use, with little awareness of their susceptibility to attacks. A severe shortage of cyber skills, with one in three positions vacant, has hindered progress. The NAO calls for urgent action, including a comprehensive cyber strategy and better recruitment to address these challenges. Furthermore, incidents like the 2024 NHS cyber attack underline the risks to public services, highlighting the need for faster, more coordinated cyber resilience. The government is urged to close gaps in cyber capabilities to avoid devastating consequences for national security and public services.

MASSIVE IOT DATA BREACH EXPOSES 2.7 BILLION RECORDS, RAISING SMART HOME SECURITY FEARS

A significant data breach has compromised approximately 2.7 billion records associated with Mars Hydro, a Chinese manufacturer of Internet of Things (IoT) devices such as LED lights and hydroponics equipment. The breach, attributed to an unsecured database, has raised critical concerns about the security of smart home devices and the potential risks to consumers. According to reports from ZoneAlarm and Infosecurity Magazine, the incident underscores the vulnerabilities present in IoT ecosystems.

The exposed data includes usernames, email addresses, device information, and logs of activity. The vulnerability stemmed from misconfigured cloud storage, leaving sensitive information publicly accessible without authentication. Cybersecurity researchers discovered the issue and alerted the company; however, the duration of exposure and whether cybercriminals accessed the data remain unclear.

This incident highlights major security weaknesses within the smart home industry, where convenience often takes precedence over security. The vast amount of exposed data could be exploited for phishing scams, unauthorised control of smart devices, and even physical security risks.

Users of Mars Hydro devices are urged to change their passwords immediately and Infosecurity Magazine recommends enabling two-factor authentication (2FA) as an additional layer of security to prevent unauthorised access.

Keeping smart home devices and software updated is crucial, as regular security patches can protect against vulnerabilities. Additionally, consumers should review the privacy settings of their IoT devices and disable unnecessary features that collect personal information.

LAZARUS GROUP EXPLOITS LINKEDIN TO DEPLOY CRYPTOCURRENCY-STEALING MALWARE

In February, it was reported that the North Korean state-sponsored hacking collective, known as the Lazarus Group, has intensified its cyber espionage efforts by targeting job seekers on LinkedIn with sophisticated malware designed to steal cryptocurrency. Reports from CSO Online and SOCRadar indicate that the group is exploiting professional networking platforms to deceive unsuspecting victims.

The attackers pose as recruiters offering lucrative job opportunities. Victims receive seemingly legitimate job descriptions embedded with malicious code. Upon opening these documents, the malware is activated, compromising the user's system and enabling the theft of cryptocurrency assets. This tactic allows the hackers to bypass traditional security measures and gain access to sensitive financial data.

This campaign is part of a broader strategy by the Lazarus Group to infiltrate organisations and individuals involved in the cryptocurrency industry. Cybersecurity experts urge job seekers to exercise caution when engaging with unsolicited job offers, verify recruiters' identities, and avoid downloading attachments from unknown sources.

PALO ALTO NETWORKS FIREWALLS UNDER ATTACK AS HACKERS EXPLOIT CRITICAL VULNERABILITIES

Palo Alto Networks has confirmed active exploitation of multiple firewall vulnerabilities, including CVE-2025-0108, which allows unauthorised access to management interfaces. According to SecurityWeek, attackers began targeting the flaw within a day of its disclosure.

Infosecurity Magazine reports that hackers are chaining this vulnerability with others, such as CVE-2024-9474 and CVE-2024-0012, to achieve remote code execution. This poses a serious risk to organisations using these firewalls.

Palo Alto Networks urges users to apply patches immediately, restrict internet exposure of management interfaces, and strengthen access controls. The incident highlights the need for continuous security updates to defend against evolving cyber threats.

UK HEALTHCARE PROVIDER FACES $2 MILLION RANSOM DEMAND FOLLOWING CYBERATTACK

HCRG Care Group, a UK-based private health and social services provider, has reportedly been targeted by the Medusa ransomware gang, resulting in a ransom demand of £1.6 million ($2 million). The cybercriminals claim to have exfiltrated approximately 2.275 terabytes of data, including sensitive internal records such as passport and driving licence scans, birth certificates, background checks, and staff rotas.

Unlike typical ransomware attacks where data is encrypted to disrupt operations, the Medusa group did not encrypt HCRG's data, allowing the organisation to continue its services without interruption. However, the threat actors have warned that they will publicly release the stolen information if the ransom is not paid by February 27. They have also offered to delay the data leak for a fee of £8,000 per day to facilitate ongoing negotiations.

In response, HCRG Care Group has implemented immediate containment measures and engaged external forensic specialists to investigate the incident. A spokesperson for the organisation stated that no suspicious activity has been observed since these measures were enacted, and services continue to operate safely. Patients with appointments are advised to attend as scheduled.

This incident underscores the escalating threat of ransomware attacks targeting the healthcare sector, with cybercriminals increasingly seeking to monetise stolen data through extortion.

CYBER GLOSSARY

2-step verification (2SV): Sometimes called 2FA or MFA is a second way to confirm your identity to help keep your personal and financial information from being compromised or stolen.

Anti-virus software: Designed to identify and remove computer viruses, other malware and spyware on a device or IT system. To be effective, it should be kept up-to-date with the latest anti-virus signatures and definitions.

Backdoor: A backdoor is a method of avoiding normal authentication on a device. They are often used for securing remote access to a computer, or obtaining access to plaintext in cryptographic systems

Common Vulnerabilities and Exposures (CVE): The Common Vulnerabilities and Exposures (CVE) system provides a reference-method for publicly known information-security vulnerabilities and exposures.

Cryptocurrency: A cryptocurrency is a digital asset that is designed to act as an exchange medium. They use cryptography to verify and secure transactions, control the creation of new assets and protect the identity of asset holders.

Dark web: A collection of thousands of websites which are not indexed by conventional search engines. They often use anonymity tools, like the Tor network, to hide their IP address and preserve the anonymity of the creators and visitors.

Encryption: A method to scramble a message, file or other data and turn it into a secret code using an algorithm (complex mathematical formula). The code can only be read using a key or other piece of information (such as a password) which can decrypt the code.

Firewall: A security system that monitors and controls traffic between an internal network (trusted to be secure) and an external network (not trusted). It is generally considered insufficient against modern cyber threats.

General Data Protection Regulation - GDPR: The General Data Protection Regulation (GDPR) 2016/679 is a European Union regulation covering data protection and individual privacy rights. It was introduced in April 2018 and enforced on May 25 2018.

Hacker: A hacker is a computer and networking attacker who systematically attempts to penetrate a computer system or network using tools and attack methods to find and exploit security vulnerabilities.

IP address: An IP address (Internet Protocol Address) is a label assigned to computer devices. An IP address is essential for Internet Protocol communication.

Keylogging: Keylogging, also known as keystroke logging or keyboard capture, is the action of recording, often secretly, the keys struck on a keyboard.

Malware: Malware is malicious or hostile software used to disrupt, damage or compromise a computer system or network

Patch management: Patch management covers acquiring, testing and installing multiple patches (manufacturer released code changes) to a computer system or application. Firmware and software vendors release patches to fix defects, change functionality and to address known security vulnerabilities.

Phishing: Phishing is a type of fraud in which the attacker attempts to steal sensitive data such as passwords or credit card numbers, via social engineering.

Ransomware: A type of malware that prevents access to the target's computer system or data until a ransom is paid to the attacker.

Smishing: A type of phishing attack that uses text messages (or other types instead of mobile messaging such as MMS or IM services) instead of email messages.

Social engineering: An attack method that tricks people into breaking normal security procedures by masquerading as a reputable entity or person in email, IM or other communication channels.

Vulnerability: A vulnerability is a weakness that allows an attacker to compromise security (integrity, confidentiality or availability).

ABOUT US

TThe Cyber Security Centre for the Isle of Man (CSC) is dedicated to enhancing the cyber resilience of organisations and individuals across the island. As a public-facing entity, the CSC provides comprehensive advice, guidance, and practical support to both residents and businesses.

The CSC is committed to bolstering cyber defences by offering tailored solutions, resources, and educational programmes. Its primary focus lies in empowering Island-based entities and individuals with the necessary knowledge and tools to effectively safeguard against cyber threats.

Through proactive initiatives, including targeted advisory notices, vulnerability scanning, and awareness campaigns, the CSC aims to elevate the overall cyber awareness and preparedness of the Isle of Man community. By fostering a culture of vigilance and best practices, the CSC aims to fortify the cyber resilience of organisations and individuals, ensuring a safer digital environment for all.

Disclaimer

The material in this document is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances. OCSIA accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

Open Government Licence

Cyber Security Centre for the Isle of Man

a part of the Office of Cyber-Security & Information Assurance

csc.gov.im
cyber@gov.im
01624 685557

Office of Cyber-Security & Information Assurance
2nd Floor
Former Lower Douglas Police Station
Fort Street
Douglas
Isle of Man
IM1 2SR

T: +44 1624 685557

Isle of Man Government
Reiltys Ellan Vannin